UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/237,003	09/27/2005	James A. Roskind	PB-034	5151

85853 7590 10/12/2011

Aaron Emigh
762 Judith Court
Incline Village, NV 89451

EXAMINER	
SIMS, JING F	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
10/12/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	11/237,003	ROSKIND ET AL.	
	Examiner	Art Unit	
	JING SIMS	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 July 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,2,4-10,12-14,24 and 25* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,2,4-10,12-14,24 and 25* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. In view of the Appeal Brief filed on July 19, 2011, PROSECUTION IS HEREBY REOPENED. New Grounds of rejection are set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) initiate a new appeal by filing a notice of appeal under 37 CFR 41.31 followed by an appeal brief under 37 CFR 41.37. The previously paid notice of appeal fee and appeal brief fee can be applied to the new appeal. If, however, the appeal fees set forth in 37 CFR 41.20 have been increased since they were previously paid, then appellant must pay the difference between the increased fees and the amount previously paid.

A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

Claim Rejections - 35 USC § 101

2. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 14 is directed to non-statutory subject matter. The decision on whether this claim is statutory or not would depend on whether or not the specification defines "a computer readable storage medium" as not being a signal otherwise the ordinary

meaning in the art that "a computer readable storage medium" can be a signal is rule and the claim is not statutory.

The broadest reasonable interpretation of a claim drawn to a computer readable medium (also called machine readable medium and other such variations) typically covers forms of non-transitory tangible media (or non-transitory media) and transitory propagating signals per se in view of the ordinary and customary meaning of computer readable media, particularly when the specification is **silent** (or absent of a controlling definition in the specification). See MPEP §2111.01. When the broadest reasonable interpretation of a claim covers a signal per se, the claim must be rejected under 35 U.S.C. § 101 as covering non-statutory subject matter. See In re Nuijten, 500 F.3d 1346, 1356-57 (Fed. Cir. 2007) (transitory embodiments are not directed to statutory subject matter); see Interim Examination Instructions for Evaluating Subject Matter Eligibility under 35 U.S.C. § 101, Aug. 24, 2009; p. 2 and Official Gazette Notice link:

http://www.uspto.gov/web/offices/com/sol/og/2010/week08/TOC.htm#ref20 or Subject Matter Eligibility of Computer Readable Media (26Jan2010) 1351 OG 21223FEB2010

Non acceptable

variations may be "machine (or computer) readable (or accessible or usable) storage medium", "recording medium", "tangible (or physical) machine (or computer) readable (or accessible or usable) storage medium"

Note: a "tangible medium" includes transitory propagating signals as the modifier/adjective "tangible" means capable of being touched or perceived and signal (e.g. sound) can be perceived.

Possible fix:

Amend the claimed term to: "non-transitory", "computer usable memory", or "computer usable storage memory", "computer readable memory", "computer readable device", (i.e. any variations thereof, where **"media" or "medium"** is replaced by "**device**" or "**memory**") or adding "wherein the medium is not a signal".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1, 2, 4-10, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Liang (US 7287278 B2) in view of Yan et al. (US 2005/0033987 A1, hereinafter, Yan).**

As per claim 1, Liang discloses "a method for protecting a network, comprising":

"detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present), "quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a

virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

Liang discloses detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device; however, Liang does not discloses detecting the insecure condition includes contacting a trusted computing based associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness.

Yan discloses **detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module** (e.g., [0019], [0055], [0077]: seeking to know the state of the computing environment inside TPS 100 depends on the value of the integrity metrics; wherein a trusted computing base corresponding with a mechanism that provide the security related integrity metrics checking to the computing system), and **the response includes a valid digitally signed attestation of cleanliness** (e.g., [0055], [0077]: TPM 130 proclaims its trustworthiness by signing data using one of its identities, the signature key is known only to TPM 130 and is the private key of a key pair).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device as described by Liang and add the insecure condition includes contacting a trusted computing base associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness as taught by Yan because it would

improve trust in one platform with eventual trust provide by the trusted computing platform and promotes the concept of a trusted subsystem and chains of trust between such subsystems (see Yan, [0003]).

As per claim 2, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, and determining that an available patch has not been installed" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 4, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed" (col. 8 line 55-64, if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 5, Liang discloses "a method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system" (col. 17, line 47-55, identifying a new client device to e added to the network. Identification includes identifying the type of system, resident operating system etc. In col. 18, line 4-7, if the new client has been determined that proper anti-virus policies and protocols are not in place, then all access to all addresses except to that of an anti-virus software installation server are blocked. Liang teaches the client need to meet certain safety policies and protocols to access the network. The initial startup after installation of the operating system is the configuration of the system; therefore, it is the policies and protocols).

As per claim 6, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular those data packets found to be virus-free are sent back to the network traffic flow).

As per claim 7, Liang discloses "a method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host" (col. 15, line 47-57, the security module has determined that a particular data packets deemed more likely to be affected are passed directly to the file scan module. A data packet is always has its purpose to request service from the destination network and it is usually not address to a remediation host).

As per claim 8, Liang discloses "a method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 9, Liang discloses "a system for protecting a network, comprising: a processor configured to":

"detect an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor monitors activities of network, detecting abnormal events from other computers that on the network. Liang also describes virus monitors can be a stand alone server computer in col. 7, line 15-21), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems)

"and permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak) "and a memory coupled to the processor and configured to provide instructions to the processor" (col. 7, line 15-21, virus monitors can be a stand alone server computer. Every stand alone computer includes memory and processor).

Liang discloses detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device; however, Liang does not discloses detecting the insecure condition includes contacting a trusted computing based associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness.

Yan discloses **detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module** (e.g., [0019], [0055], [0077]: seeking to know the state of the computing environment inside TPS 100 depends on the value of the integrity metrics; wherein a trusted computing base corresponding with a mechanism that provide the security related integrity metrics checking to the computing system), and **the response includes a valid digitally signed attestation of cleanliness** (e.g., [0055], [0077]: TPM 130 proclaims its trustworthiness by signing data using one of its identities, the signature key is known only to TPM 130 and is the private key of a key pair).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify detecting an insecure condition in a client computing

device and receiving an response of the cleanliness of the client computing device as described by Liang and add the insecure condition includes contacting a trusted computing base associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness as taught by Yan because it would improve trust in one platform with eventual trust provide by the trusted computing platform and promotes the concept of a trusted subsystem and chains of trust between such subsystems (see Yan, [0003]).

As per claim 10, Liang discloses "a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data" (col. 3, line 7-9, scanning for abnormal network packets at protocols layers) "checking a configuration or setting, determining whether a security data is up to date, determining whether a security software is installed, detecting anomalous network traffic, determining that an available patch has not been installed, and querying the first host for a cleanliness assertion" (col. 8, line 27-32, and line 49-64, virus monitor is queried in order to determine if that client device has the appropriate and proper anti-virus software; virus monitor sends query to each of the client devices requesting confirmation of each has installed the appropriate anti-virus software. Upon receiving the query, the client devices checks that proper software is indeed present (based upon the policies in the OPP files), if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems).

As per claim 12, Liang discloses "a system as recited in claim 9, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed" (col. 7, line 25-36, the controller includes a rules engine used to store and source of detection rules for detecting computer viruses and an outbreak prevention policy distribution and execution engine that provides a set of anti-virus policies, protocols, and procedures suitable for use by a system administrator for both preventing viral outbreaks and repairing any subsequent damage caused by a viral outbreak. Liang also discloses the policies, protocols and procedures can be periodically updated. Checking initial startup after installation of an OS is regular procedure to perform for securing of a computer, therefore the rules, polices, or procedures that Liang described include that checking initial startup after installation of an OS).

As per claim 13, Liang discloses "a system as recited in claim 9, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition" (column 8, line 39-48, in situations where a client device is found not have the appropriate anti-virus software installed, virus monitor will target client device and block any traffic to/from the target client device and all other addresses until such time as the appropriate software has been installed).

As per claim 14, Liang discloses "a computer program product for protecting a network, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for" (col. 3, line 44-45, and line 59-67, a computer program project for monitoring a network for computer viruses):

"detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network" (col. 9, line 49-52, virus monitor activities of network, detecting abnormal events from other computers that on the network), "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within first host" (col. 8, lines 49-53, send a query to client device requesting confirmation);

"and determining whether the response includes a valid digitally signed attestation of cleanliness (col. 8, lines 53-55, upon receiving the query, client device checks for confirmation; lines 66-67, the encryption thereof could be used)";

"when it is determined that the response does not include a valid digitally signed attestation of cleanliness" (col. 8, lines 55-59, client device is determined that either no proper software is present),

"quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network" (col. 9, line 58-67, quarantine affected segments of network in order to prevent a spread of the virus. Inoculate other computers in the network. In col. 8 line 55-64, Liang also teaches if client device is in an insecure condition, the client device is redirected to the anti-virus software installation server and no other. Until the proper software has been installed, the client device will be prevented from communication with other systems);

"and permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition" (col. 9, line 61-67, distribute a virus cleaning agent to the affected segment, and repair any damage caused by virus outbreak).

Liang discloses detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device; however, Liang does not discloses detecting the insecure condition includes contacting a trusted computing based associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness.

Yan discloses **detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module** (e.g., [0019], [0055], [0077]: seeking to know the state of the computing environment inside TPS 100 depends on the value of the integrity metrics; wherein a trusted computing base corresponding with a mechanism that provide the security related integrity metrics checking to the computing system), and **the response includes a valid digitally**

signed attestation of cleanliness (e.g., [0055], [0077]: TPM 130 proclaims its trustworthiness by signing data using one of its identities, the signature key is known only to TPM 130 and is the private key of a key pair).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify detecting an insecure condition in a client computing device and receiving an response of the cleanliness of the client computing device as described by Liang and add the insecure condition includes contacting a trusted computing base associated with a trusted platform module, and the response includes a valid digitally signed attestation of cleanliness as taught by Yan because it would improve trust in one platform with eventual trust provide by the trusted computing platform and promotes the concept of a trusted subsystem and chains of trust between such subsystems (see Yan, [0003]).

5. **Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of Lewis**.

As per claim 24, claim 1 is incorporated and, Lewis discloses further comprising:

receiving a service request sent by the first host; serving a quarantine notification page to the first host if the service request comprises a web server request" (page 8, [0083], lines 20-22, wherein a quarantine notification page corresponding to fix-up page on QS, QS stands for quarantine server);

"and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host" (page 8, [0082], the purpose is to prevent the unsafe machine from talking to any other network node except for the few select severs it can use to update it compliance with network security policy; [0083], whenever the client performs name resolution on any address, it will receive the IP of quarantine server. This way any client will be redirected to fix-up page on quarantine server).

Liang and Lewis are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host as described by Liang and add the host request service including DNS and other requests as taught by Lewis because it would be added more detailed of the normal services that request from a host to a server in a secured network.

6. **Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over Liang in view of McElhaney, Jr. et al. (US patent no. US 6,823,479 B1) (hereinafter McElhaney).**

As per claim 25, in claim 1 is incorporated, and McElhaney discloses "performed at an Internet service provider" (col. 1, line 26-35, ISP provides test tools to protect subscribers by isolate the damaged root).

Liang and McElhaney are analogous art because of they are from the same field of endeavor of improve a security of network by quarantining infected hosts.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the inoculation of computer host in a distributed network as described by Liang and add the distributed network also can an ISP as taught by McElhaney because it would be logically expanded the network to an distributed network work such as an Internet Service Provider.

Examiner Notes

7. Examiner has pointed out particular references contained in the prior arts of record and in the body of this action for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. Applicant should consider the entire prior art as applicable to the limitations of the claims. It is respectfully requested from the applicant, in preparing for response, to consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior arts or disclosed by the Examiner.

Conclusion

8. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jing Sims whose telephone number is (571)270-7315. The examiner can normally be reached on 9:00am-5:00pm EST, Mon-Thu.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jing Sims/
Examiner, Art Unit 2437
/Eleni A Shiferaw/

Supervisory Patent Examiner, Art Unit 2437